# ŠIFROVACÍ METODA ZALOŽENÁ NA FRAKTÁLNÍ KOMPRESI

Tomáš Grísa

Abstrakt. Tento článek se zabývá teoretickými principy fraktální komprese a využitím modifikovaného algoritmu fraktální komprese pro symetrickou kryptografii. Kompaktní matematická teorie a vlastní algoritmus navržené symetrické šifry (Fractal Compression Based Cryptosystem - FCBC) jsou zde prezentovány. Tato práce také obsahuje příklad ilustrující praktické využití této šifry a její různé modifikace.

## 1. Úvod

V posledních letech se ukázalo, že teorii fraktálů lze využít v mnoha teoretických i praktických oborech. Příkladem může být fraktální komprese obrazu využívající *systém iterovaných funkcí (IFS)* a *segmentovaný systém iterovaných funkcí (PIFS)*, kterou v roce 1987 navrhl Barnsley (viz. [1], [2]). Využil soběpodobnost pro obrazovou kompresi tak, že atraktor PIFS je aproximací původního obrazu. Avšak hledání soběpodobných částí v rastrovém obraze je výpočetně náročné.

Další zajímavou oblastí, kde lze aplikovat teorii fraktálů, je kryptografie. Tento text se zabývá právě touto oblastí. Popisuje modifikovaný reverzní algoritmus fraktální komprese použitý pro symetrickou šifru (FCBC), která je hlavním výsledkem této práce. V navržené šifře se PIFS iterativně aplikuje na libovolnou zprávu vhodné délky. Atraktorem tohoto PIFS je pak výsledná zašifrovaná zpráva. Klíč a zpráva k zašifrování jsou použity jako koeficienty daného PIFS. Zašifrovaná zpráva je tedy v jistém smyslu soběpodobná. Pokud známe klíč, můžeme pomocí jednoduchých výpočtů obdržet původní zprávu.

V textu se předpokládá znalost pojmů *metrický prostor, posloupnost, konvergence posloupnosti, cauchyovská posloupnost, úplný metrický prostor* a *kompaktní množina*.

## 2. Matematické principy

**Definice 2.1.** Nechť $(\mathcal{M}, d)$ je metrický prostor a $T : \mathcal{M} \to \mathcal{M}$. Zobrazení $T$ nazveme:

- *lipschitzovské* právě tehdy, když existuje konstanta $l > 0$ taková, že:

$$d\left(T\left(x\right), T\left(y\right)\right) \leq l \cdot d\left(x, y\right) , \qquad \forall x, y \in \mathcal{M} ,$$

2010 *MSC*. Primární 94A60; Sekundární 11T71.

*Klíčová slova.* Fraktální komprese, symetrický kryptosystém, Fractal Compression Based Cryptosystem, FCBC.

Práce byla podporována projektem A-Math-Net – Síť pro transfer znalostí v aplikované matematice (CZ.1.07/2.4.00/17.0100).

- *kontraktivní* právě tehdy, když existuje konstanta $0 < c < 1$ taková, že:

$$d\left(T\left(x\right), T\left(y\right)\right) \leq c \cdot d\left(x, y\right), \qquad \forall x, y \in \mathcal{M},$$

- *neexpanzivní* právě tehdy, když:

$$d\left(T\left(x\right), T\left(y\right)\right) \leq d\left(x, y\right), \qquad \forall x, y \in \mathcal{M}.$$

**Tvrzení 2.2.** *Jestliže je zobrazení $T : \mathcal{M} \to \mathcal{M}$ lipschitzovské, potom je i spojité.*

*Důkaz.* Předpokládejme $T$ spojité s lipschitzovým koeficientem $l$. Nechť $\varepsilon > 0$. Pokud $|x - y| < \varepsilon/l$, dostáváme že

$$|T(x) - T(y)| \leq l|x - y| < l \cdot \frac{\varepsilon}{l} = \varepsilon,$$

kde první nerovnost je ekvivalentní s lipschitzovou podmínkou. Pokud je tedy $\varepsilon$ libovolné, pak $T$ je spojité. □

**Definice 2.3.** Bod $x^* \in \mathcal{M}$ se nazývá *pevným bodem zobrazení* $T : \mathcal{M} \to \mathcal{M}$ právě tehdy, když

$$T\left(x^*\right) = x^* = \lim_{n \to \infty} T^n\left(x^*\right).$$

**Věta 2.4. (Banachova věta o pevném bodu kontraktivního zobrazení)** *Buď $\mathcal{M}$ úplný metrický prostor a $T : \mathcal{M} \to \mathcal{M}$ kontraktivní zobrazení. Potom $T$ má právě jeden pevný bod.*

*Důkaz.* Zvolme libovolné $x \in \mathcal{M}$. Potom pro $n > m$ platí

$$d\left(T^m\left(x\right), T^n\left(x\right)\right) < c \cdot d\left(T^{m-1}\left(x\right), T^{n-1}\left(x\right)\right) < c^m \cdot d\left(x, T^{n-m}\left(x\right)\right). \tag{2.1}$$

Dále využijme trojúhelníkovou nerovnost:

$$\begin{aligned} d\left(x, T^k\left(x\right)\right) &\leq d\left(x, T^{k-1}\left(x\right)\right) + d\left(T^{k-1}\left(x\right), T^k\left(x\right)\right) \\ &\leq d\left(x, T\left(x\right)\right) + d\left(T\left(x\right), T\left(T\left(x\right)\right)\right) + \ldots + d\left(T^{k-1}\left(x\right), T^k\left(x\right)\right) \\ &\leq \left(1 + c + \ldots + c^{k-2} + c^{k-1}\right) \cdot d\left(x, T\left(x\right)\right) \\ &\leq \frac{1}{1-c} \cdot d\left(x, T\left(x\right)\right). \end{aligned} \tag{2.2}$$

Nyní můžeme přepsat výraz 2.1 následovně:

$$d\left(T^m\left(x\right), T^n\left(x\right)\right) < \frac{c^m}{1-c} \cdot d\left(x, T\left(x\right)\right).$$

Jestliže $c < 1$, potom můžeme vzít levou stranu výrazu libovolně malou, pokud jsou $n$ a $m$ dostatečně velká. To znamená, že posloupnost $x, T\left(x\right), T\left(T\left(x\right)\right), \ldots$ je cauchyovská. Pokud je $\mathcal{M}$ úplný metrický prostor, potom bod $x^* = \lim_{n\to\infty} T^n\left(x\right)$ leží v $\mathcal{M}$. Nyní podle tvrzení 2.2 platí, že pokud je $T$ kontraktivní, je $T$ zároveň spojité. Tudíž $T\left(x^*\right) = T\left(\lim T^n\left(x\right)\right) = \lim T^{n+1}\left(x\right) = x^*$.
Jednoznačnost dokažme následovně: předpokládejme, že $x_1^*$ a $x_2^*$ jsou dva pevné body. Potom $d\left(T\left(x_1^*\right), T\left(x_2^*\right)\right) = d\left(x_1^*, x_2^*\right)$, zároveň ale platí $d\left(T\left(x_1^*\right), T\left(x_2^*\right)\right) \leq c \cdot d\left(x_1^*, x_2^*\right)$. Tím dostáváme spor. □

**Věta 2.5. (Kolážová věta)** *Buď $T$ kontraktivní zobrazení s koeficientem kontrakce $c$, a $x^*$ pevným bodem zobrazení $T$. Potom platí:*

$$d(x, x^*) \leq \frac{1}{1-c} \cdot d(x, T(x))$$

*Důkaz.* Věta plyne z výrazu 2.2, pokud $k$ jde k nekonečnu. □

**Definice 2.6.** Buď $T$ lipschitzovské zobrazení. Pokud existuje $n \in \mathbb{N}$ takové, že $T^n$ je kontraktivní, pak zobrazení $T$ nazveme *podmíněně kontraktivní*. Exponent $n$ nazveme *exponentem podmíněné kontrakce.*

**Věta 2.7. (Zobecněná kolážová věta)** *Buď $T$ podmíněně kontraktivní s exponentem podmíněné kontrakce $n$, potom toto zobrazení má právě jeden pevný bod $x^*$, kterého dosáhneme pro libovolné $x$ následovně:*

$$x^* = T(x^*) = \lim_{k \to \infty} T^k(x).$$

*Potom platí:*

$$d(x, x^*) \leq \frac{1}{1-c} \frac{1-l^n}{1-l} \cdot d(x, T(x)),$$

*kde $c$ je koeficient kontrakce $T^n$, a $l$ je lipschitzovým koeficientem $T$.*

*Důkaz.* Viz. [2], str. 36 □

**Definice 2.8.** Pokud je $(\mathcal{M}, d)$ úplný metrický prostor, potom *systémem iterovaných funkcí (IFS)* nazýváme konečnou množinu kontraktivních zobrazení $F = \{w_1, w_2, ..., w_n\}$ definovaných na $\mathcal{M}$.

**Definice 2.9.** Pro metrický prostor $(\mathcal{M}, d)$ označme $H(\mathcal{M})$ systém všech neprázdných kompaktních podmnožin $\mathcal{M}$. Potom zobrazení $d_h : H(\mathcal{M}) \times H(\mathcal{M}) \to \mathbb{R}_0^+$ definované předpisem

$$d_h(A, B) = \max\{\sup_{a \in A} \inf_{b \in B} d(a, b), \sup_{b \in B} \inf_{a \in A} d(a, b)\}$$

pro neprázdné $A, B \subseteq \mathcal{M}$ nazveme *Hausdorffovou vzdáleností.* Ta splňuje axiomy metriky, tudíž $(H(\mathcal{M}), d_h)$ tvoří metrický prostor.

**Věta 2.10. (IFS věta)** *Je-li $(\mathcal{M}, F)$ systémem iterovaných funkcí, potom transformace $\mathcal{W} : H(\mathcal{M}) \to H(\mathcal{M})$, pro kterou platí*

$$\mathcal{W}(B) = \bigcup_{i=1}^{n} w_i(B)$$

*pro všechna $B \in H(\mathcal{M})$, je kontraktivním zobrazením na $(H(\mathcal{M}), d_h)$ s koeficientem kontrakce $c = \max\{c_1, ..., c_n\}$. Pak tato transformace má jediný pevný bod $A \in H(\mathcal{M})$, který vyhovuje rovnici $A = \mathcal{W}(A)$ a je dán limitou $A = \lim_{i \to \infty} \mathcal{W}^i(B)$ pro libovolné $B \in H(\mathcal{M})$.*

*Důkaz.* Viz. [2], str. 34 □

**Definice 2.11.** Buď $\mathcal{M}$ úplný metrický prostor, dále buď $D_i \subset \mathcal{M}$ pro $i = 1, ..., n$. Potom *segmentovaným systémem iterovaných funkcí (PIFS)* nazýváme množinu kontraktivních zobrazení $w_i : D_i \to \mathcal{M}$, pro $i = 1, ..., n$.

*Poznámka* 2.12. PIFS má (stejně jako v případě pro IFS) právě jeden pevný bod. Pokud budeme navíc uvažovat, že PIFS obsahuje i podmíněně kontraktivní, popřípadě neexpanzivní zobrazení, dá se ukázat, že i v tomto případě má toto PIFS právě jeden pevný bod. Viz. [3].

## 3. Algoritmus

**Definice 3.1.** Řekneme, že $q$ je *podíl celočíselného dělení dvou celých čísel* $a \in \mathbb{N}_0, b \in \mathbb{N}$, pokud splňuje

$$a = b \cdot q + r\,, \qquad q \in \mathbb{N}_0, r \in \langle 0, |q|) \cap \mathbb{N}_0,$$

potom celočíselné dělení značíme $a \text{ div } b = q$ a zbytek po tomto celočíselném dělení značíme $a \bmod b = r$.

**Tvrzení 3.2.** *Mějme následující celočíselné dělení*

$$a \ div\ b, a \in \mathbb{N}_0, b \in \mathbb{N} - \{1\}.$$

*Potom v* $\mathbb{N}_0$ *s klasickou metrikou je toto celočíselné dělení neexpanzivní, a podmíněně kontraktivní.*

**Definice 3.3.** Definujme *zprávu* $\mathcal{M}$ jako konečnou posloupnost čísel z omezeného intervalu přirozených čísel. Délku zprávy (počet prvků této posloupnosti) označme $|\mathcal{M}|$. $N-tý$ prvek zprávy označme $m_n$.

**Definice 3.4.** Definujme *klíč* $\mathcal{K}$ jako konečnou posloupnost celočíselných dvojic $[\delta, \kappa]$, kde $\delta$ je z omezeného intervalu přirozených čísel a $\kappa \in \{2, 3, ..., 11\}$. Délku klíče (počet celočíselných dvojic této posloupnosti) označme $|\mathcal{K}|$. První prvek $n-té$ celočíselné dvojice klíče označme $\delta_n$, druhý prvek této dvojice potom $\kappa_n$.

**Algoritmus:**
Mějme zprávu $\mathcal{A}$ délky $|\mathcal{A}|$ a klíč $\mathcal{K}$ délky $|\mathcal{K}|$. Dále mějme libovolnou zprávu $\mathcal{B}$ délky $|\mathcal{B}| = |\mathcal{A}|$.

1. Vytvořme novou (pomocnou) zprávu $\mathcal{E}$ délky $|\mathcal{E}| = |\mathcal{A}|$ podle následujícího předpisu

$$e_n = \left(\left(b_{((n+\delta_j-1) \bmod |\mathcal{E}|)+1}\right) \text{ div } \kappa_j\right) + a_n, \qquad j = ((n-1) \bmod |\mathcal{K}|) + 1. \quad (3.1)$$

2. Pokud

$$\sum_{i=1}^{|\mathcal{A}|} |b_i - e_i| = 0, \quad (3.2)$$

vrať $\mathcal{E}$ a ukonči výpočet. V opačném případě $\mathcal{B} = \mathcal{E}$ a jdi na bod #1.

Nyní jsme schopni rekonstruovat zprávu $\mathcal{A}$ podle následujícího předpisu

$$a_n = b_n - \left(\left(b_{((n+\delta_j-1) \bmod |\mathcal{E}|)+1}\right) \text{ div } \kappa_j\right), \qquad j = ((n-1) \bmod |\mathcal{K}|) + 1. \quad (3.3)$$

*Poznámka* 3.5. Z předpokladů plyne, že $\kappa$ musí splňovat podmínku $\kappa \geq 2$. Avšak pokud vezmeme $\kappa$ příliš velké, potom bude výsledek celočíselného dělení v algoritmu relativně malý. Tedy zašifrovaná zpráva by se příliš nelišila od zprávy původní. Proto v tomto algoritmu uvažujme $\kappa \in \{2, 3, ..., 11\}$.

**Lemma 3.6.** *Nechť $\mathcal{A}$ je zpráva, $\mathcal{K}$ je klíč a $\mathcal{E}$ je odpovídající zašifrovaná zpráva. Potom pro daný klíč $\mathcal{K}$ je zašifrovaná zpráva $\mathcal{E}$ jednoznačně určena, a je možno jí dosáhnout pouze z $\mathcal{A}$.*

*Důkaz.* Nechť $\mathcal{A}$, $\mathcal{B}$ jsou dvě navzájem odlišné zprávy stejné délky, a nechť $\mathcal{K}$ je libovolný klíč. Předpokládejme, že obě ze zpráv $\mathcal{B}$ a $\mathcal{A}$ mohou být zašifrovány stejným klíčem $\mathcal{K}$ do totožné zprávy $\mathcal{E}$. Potom pro každé $n$ musí platit:

$$e_n = \left(\left(e_{((n+\delta_j-1) \bmod |\mathcal{E}|)+1}\right) \operatorname{div} \kappa_j\right) + a_n$$
$$e_n = \left(\left(e_{((n+\delta_j-1) \bmod |\mathcal{E}|)+1}\right) \operatorname{div} \kappa_j\right) + b_n,$$
$$j = ((n-1) \bmod |\mathcal{K}|) + 1.$$

Avšak z předpokladu $\mathcal{A} \neq \mathcal{B}$ plyne, že zde existuje alespoň jedno $n$ takové, pro které platí $a_n \neq b_n$. Tudíž dostáváme spor. □

**Příklad 3.7.** Mějme zprávu $\mathcal{A} = \{50, 37, 85, 12, 69, 23, 52, 71, 49, 5\}$ délky $|\mathcal{A}| = 10$. Dále mějme klíč $\mathcal{K} = \{[35, 5], [9, 2], [73, 6]\}$ délky $|\mathcal{K}| = 3$ a zprávu $\mathcal{B} = \{0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}$ délky $|\mathcal{B}| = 10$. Nyní vytvořme podle 3.1 novou zprávu $\mathcal{E}$ délky $|\mathcal{E}| = 10$.

$$\begin{aligned} e_1 &= ((b_6) \operatorname{div} 5) + a_1 = (0 \operatorname{div} 5) + 50 = 50 \\ e_2 &= ((b_1) \operatorname{div} 2) + a_2 = (0 \operatorname{div} 2) + 37 = 37 \\ &\vdots \\ e_{10} &= ((b_5) \operatorname{div} 5) + a_{10} = (0 \operatorname{div} 5) + 5 = 5 \end{aligned}$$

Dostali jsme tedy zprávu $\mathcal{E} = \{50, 37, 85, 12, 69, 23, 52, 71, 49, 5\}$. Položme $\mathcal{B} = \mathcal{E}$ a vypočítejme novou zprávu $\mathcal{E}$ následovně

$$\begin{aligned} e_1 &= ((b_6) \operatorname{div} 5) + a_1 = (23 \operatorname{div} 5) + 50 = 54 \\ e_2 &= ((b_1) \operatorname{div} 2) + a_2 = (50 \operatorname{div} 2) + 37 = 62 \\ e_3 &= ((b_6) \operatorname{div} 6) + a_3 = (23 \operatorname{div} 6) + 85 = 88 \\ &\vdots \\ e_{10} &= ((b_5) \operatorname{div} 5) + a_{10} = (69 \operatorname{div} 5) + 5 = 18 \end{aligned}$$

$$\begin{aligned} \mathcal{E} &= \{54, 62, 88, 21, 75, 31, 59, 97, 55, 18\} \\ &\vdots \\ \mathcal{E} &= \{56, 64, 90, 23, 79, 32, 64, 100, 59, 20\} \\ &\vdots \\ \mathcal{E} &= \{56, 65, 90, 23, 80, 32, 64, 103, 59, 20\} \\ &\vdots \\ \mathcal{E} &= \{56, 65, 90, 23, 80, 32, 65, 103, 59, 21\} \\ &\vdots \\ \mathcal{E} &= \{56, 65, 90, 23, 80, 32, 65, 103, 59, 21\} \end{aligned}$$

Po provedení šesté iterace si můžeme všimnout, že jsme dostali stejnou zprávu $\mathcal{E}$, jako v páté iteraci. Proto šifrování ukončíme. Nyní podle 3.3 vytvořme novou zprávu $\mathcal{A}'$

$$\begin{aligned} a'_1 &= b_1 - (b_6 \text{ div } 5) = 56 - (32 \text{ div } 5) = 56 - 6 = 50 \\ a'_2 &= b_2 - (b_1 \text{ div } 2) = 65 - (56 \text{ div } 2) = 65 - 28 = 37 \\ a'_3 &= b_3 - (b_6 \text{ div } 6) = 90 - (32 \text{ div } 6) = 90 - 5 = 85 \\ &\vdots \\ a'_{10} &= b_{10} - (b_5 \text{ div } 5) = 21 - (80 \text{ div } 5) = 21 - 16 = 5 \end{aligned}$$

Zpráva $\mathcal{A}' = \{50, 37, 85, 12, 69, 23, 52, 71, 49, 5\}$ je shodná s původní nezašifrovanou zprávou $\mathcal{A} = \{50, 37, 85, 12, 69, 23, 52, 71, 49, 5\}$.

V tomto příkladu si můžeme všimnout, že znaky zašifrované zprávy nabývají větších hodnot než znaky zprávy původní. V případě, že minimální hodnota v $\kappa$ je rovna číslu 2, potom maximální hodnota výstupní abecedy může být až dvojnásobná oproti maximální hodnotě abecedy vstupní (to plyne z rovnice 3.1 pokud $((n + \delta_j - 1) \mod |\mathcal{E}|) + 1 = n$ a zároveň $a_n$ je maximální hodnotou vstupní abecedy). To může působit problémy v případě, že jako zprávu k zašifrování bereme textovou zprávu převedenou do číselné reprezentace. Protože maximální hodnota výstupní abecedy může být až dvojnásobná, neměli bychom jak zpátky vyjádřit zašifrovanou zprávu v textové reprezentaci. Jedním způsobem je rozšířit původní abecedu o nové znaky (například podtržením původních znaků). Další možností je ponechat výstup v číselné reprezentaci (decimální, případně např. hexadecimální).

*Poznámka* 3.8. Pokud šifrujeme konstantní zprávu (nebo zprávu s opakující se sekvencí stejných znaků) krátkým klíčem ($|\mathcal{K}| \ll |\mathcal{M}|$), můžou se ve výsledné zašifrované zprávě vyskytovat opakující se sekvence stejných znaků (to plyne z rovnice 3.1 pokud je klíč krátký a $a_n$ je konstantní). Pro zamezení tohoto jevu by se měl použít klíč alespoň stejné délky, jako je délka zprávy. To můžeme docílit například vhodným deterministickým algoritmem pro generování klíče potřebné délky z klíče originálního. Dalším přístupem může být definování klíče jako dvě různé konečné posloupnosti ($\Delta$ buď konečná posloupnost celých čísel z intervalu $\{2, 3, ..., 11\}$ a $K$ buď konečná posloupnost z omezeného intervalu celých čísel), kde $|\Delta| = p$, $|K| = q$ a $p \neq q$. Označme $n - tý$ prvek $K$ jako $K_n$ a $n - tý$ prvek $\Delta$ jako $\Delta_n$. Nyní je v rovnici 3.1 nutno pro $e_n$ předefinovat $\kappa_j = K_{((n-1) \mod |K|)+1}$ a $\delta_j = \Delta_{((n-1) \mod |\Delta|)+1}$. Pak můžeme využít tento klíč pro zprávu délky nejvýše $p \times q$, aniž by se ve výsledné zašifrované zprávě vyskytovaly opakující se sekvence.

## 4. Závěr

Tento článek se zabýval popisem algoritmu FCBC šifry. Základní matematická teorie, popis algoritmu a jednoduchý příklad zde byly prezentovány. Samotná šifra FCBC je příbuzná k Vigenèrově šifře, ačkoli jsou jejich algoritmy odlišné. Vigenèrova šifra je symetrická substituční šifra, kde hodnota každého symbolu zprávy je posunuta o hodnotu znaku v klíči. V FCBC šifře se hodnoty znaků také posouvají, avšak o hodnotu znaku jiného (z téže zprávy), který je navíc modifikován

hodnotou znaku v klíči. Tudíž je výsledná zpráva v jistém smyslu soběpodobná. Nevýhodou této šifry může být větší maximální hodnota výstupní abecedy oproti abecedě vstupní. Navíc pro konstantní (nebo opakující se) zprávy je třeba klíč modifikovat (avšak stejný problém se vyskytuje i u Vigenèrovy šifry).

Softwarová implementace FCBC šifry, určena pouze pro ilustrativní účely, je ke stažení na adrese:

`http://fcbc.fme.vutbr.cz`

Síla FCBC šifry by měla být přibližně shodná se sílou Vigenèrovy šifry. Pro ověření tohoto tvrzení je třeba provést kryptoanalýzu FCBC. Touto tématikou by se autor rád zabýval ve svém dalším bádání.

## Reference

[1] M. R. Barnsley: *Fractals Everywhere*, Academic Press, San Diego, 1988.
[2] Y. Fisher: *Fractal Image Compression: Theory and Application*, Springer Verlag, New York, 1995.
[3] S. K. Mitra, C. A. Murthy: *Mathematical framework to show the existence of attractor of partitioned iterative function systems*, Pattern Recognition **33** (2000), 859–869.

Tomáš Grísa, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 616 69 Brno, Česká republika,
*e-mail*: `y115559@stud.fme.vutbr.cz`